4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/872,622	05/31/2001	Augusto C. Cardoso JR.	B2C01-0001	2287

22835 7590 09/15/2004

PARK, VAUGHAN & FLEMING LLP
508 SECOND STREET
SUITE 201
DAVIS, CA 95616

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/872,622	**Applicant(s)** CARDOSO, AUGUSTO C.
	Examiner Ronald Baum	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-25 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-25 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9/23/2002.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1- 25 are pending for examination.

2. Claims 1- 25 are rejected.

Claim Rejections - 35 USC § 112

Regarding claims 9,19, the phrase "*can* involve enabling or disabling" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-6,15-22,26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Candelore, U.S. Patent Application Publication US 2004/0151314 A1.

4. As per claim 1; "A method for remotely configuring a device across a network [and associated apparatus/network system elements, Abstract, para. 0001-0066, whereas the embodiment of fig. 7, (i.e., para. 0049 et seq.) concerned with the headend aspect of the network interface deals with the control word transfer.], comprising: receiving configuration information at the device from a remote system across the network [i.e., para. 0047-0052, whereas the

headend to de-scrambler IC constitutes the data transfer across the network]; encrypting the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices [i.e., para. 0047-0052, whereas service keys based on unique keys constitutes the 'different from keys associated with other devices']; and configuring the device by storing the encrypted configuration information in a non-volatile configuration store associated with the device [i.e., para. 0047-0052, whereas stored in encrypted form and loaded into the IC constitutes the encrypting the configuration information]: whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device [i.e., para. 0047-0052, whereas service keys based on unique keys constitutes the 'different from keys associated with other devices'].";

Further, as per claim 11; "An apparatus [This claim is the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] that facilitates remotely configuring a device across a network, comprising: an interface, at the device, that is configured to receive configuration information from a remote system across the network; an encryption mechanism that is configured to encrypt the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices; and a configuration mechanism that is configured to store the encrypted configuration information in a non-volatile configuration store associated with the device: whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device.".

5. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1, wherein receiving the configuration information involves using a secret key, which is locally stored at the

device, to decrypt the configuration information received from the remote system.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, whereas stored in encrypted form and loaded into the IC constitutes the encrypting the configuration information, and subsequent decryption of content using the control words and service keys.);

Further, as per claim 12 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] of claim 11 further comprising a decryption mechanism that is configured to use a secret key, which is locally stored at the device, to decrypt the configuration information received from the remote system through the interface.".

6. Claim 3 ***additionally recites*** the limitation that; "The method of claim 1, wherein receiving the configuration information involves using a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, whereas "The service key is unit key encrypted. It may be a public asymmetric key or secret symmetric key" constitutes the "using a public key of the remote system..." using the associated control words and service keys.);

Further, as per claim 13 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] of claim 11, further comprising a validation mechanism that is configured to use a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system,".

7. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1, wherein the device key is stored in one-time programmable memory within the device that can be programmed only once and cannot be reprogrammed.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, whereas the "unique key programmed at manufacture… written only once" constitutes "the device key is stored in one-time programmable memory within the device");

Further, as per claim 14 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] of claim 11, further comprising a one-time programmable memory within the device for storing the device key; wherein the one-time programmable memory can be programmed only once and cannot be reprogrammed.".

8. Claim 5 ***additionally recites*** the limitation that; "The method of claim 1, wherein the device uses the configuration information to control access to a stream of content in order to facilitate subscriber management.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0026-0036, 0044, 0047-0052, whereas "copy management… ", and entitlement control / management constitutes 'subscriber management".);

Further, as per claim 15 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection] of claim 11, further comprising a content screening mechanism that is configured to use the configuration information to control access to a stream of content in order to facilitate subscriber management.".

9. Claim 6 ***additionally recites*** the limitation that; "The method of claim 5, wherein the configuration information includes either a fixed key or a variable key for decompression and/or decryption of the stream of content.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, whereas "The service key is unit key encrypted. It may be a public asymmetric key or secret symmetric key" constitutes the "using a public key of the remote system..." using the associated control words and service keys, and further, whereas the "unique key programmed at manufacture... written only once" constitutes "the device key is stored in one-time programmable memory within the device" which is clearly a fixed key.);

Further, as per claim 16 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] of claim 15, wherein the configuration information includes either a fixed key or a variable key for decompression and/or decryption of the stream of content.".

10. Claim 7 ***additionally recites*** the limitation that; "The method of claim 1, wherein the device includes one of: a computer; a personal digital assistant; a network interface; a cable television interface; a satellite television interface; and a network router.". The teachings of Candelore suggest such limitations (i.e., Abstract, para. 0001-0064, whereas the device is clearly a set top cable television interface, and additionally, is described as a headend computer as part of a computer network.);

Further, as per claim 17 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection] of claim 11, wherein the device includes one of: a computer; a personal digital assistant; a network interface; a cable television interface; a satellite television interface; and a network router.".

11. Claim 8 ***additionally recites*** the limitation that; "The method of claim 1, wherein the network includes one of: a local area network; a wide area network; and a wireless network.". The teachings of Candelore suggest such limitations (i.e., Abstract, para. 0001-0064, whereas the device is clearly a set top cable television interface (i.e., part of a cable / satellite broadcast content distribution network), and additionally, is described as a headend computer as part of a computer network (i.e., WAN or Internet).);

Further, as per claim 18 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection] of claim 11, wherein the network includes one of: a local area network; wide area network; and a wireless network.".

12. Claim 9 ***additionally recites*** the limitation that; "The method of claim 1, wherein configuring the device can involve enabling or disabling the device.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0026-0036, 0044, 0047-0052, whereas "copy management...", and entitlement control / management constitutes 'enabling or disabling the device' at least insofar as content distribution is concerned.);

Further, as per claim 19 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection] of claim 11 wherein the configuration mechanism can enable and/or disable the device.".

13. Claim 10 ***additionally recites*** the limitation that; "The method of claim 1 wherein the device is embodied in an integrated circuit.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, whereas the "unique key programmed at manufacture... written only once", whereas stored in encrypted form and loaded into the IC constitutes a "device is embodied in an integrated circuit".);

Further, as per claim 20 ***additionally recites*** the limitation that; "The apparatus [This claim is the system claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection] of claim 11, further comprising an integrated circuit upon which the device is embodied.".

14. Claim 21 ***additionally recites*** the limitation that; "The apparatus of claim 11, wherein the interface is configured to support one-way communication from the remote system to the device.". The teachings of Candelore suggest such limitations (i.e., Abstract, para. 0001-0064, whereas the device is clearly a set top cable television interface (i.e., part of a cable / satellite broadcast content distribution network), and clearly is configurable to support one-way communication from the remote system.).

15. Claim 22 ***additionally recites*** the limitation that; "The apparatus of claim 11 further comprising a local interface on the device for communicating with local resources; wherein the local interface is insulated from the configuration information stored in the non-volatile configuration store, so that it is impossible to access the configuration information through the local interface.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, figures 7,8 and accompanying descriptions, whereas the various data paths into

and out of (i.e., the decoder CPU in figure 7) constitutes a "local interface" that is into versus bi-directional, insofar as I/O to the de-scrambler IC is concerned.).

16. As per claim 23; "An apparatus that facilitates remotely configuring a device across a network [and associated apparatus/network system elements, Abstract, para. 0001-0066, whereas the embodiment of fig. 7, (i.e., para. 0049 et seq.) concerned with the headend aspect of the network interface deals with the control word transfer.]; comprising: an interface, at the device, that is configured to receive configuration information from a remote system across the network [Abstract, para. 0001-0064, whereas the device is clearly a set top cable television interface (i.e., part of a cable / satellite broadcast content distribution network), and clearly is configurable to support one-way communication from the remote system.]; a decryption mechanism that is configured to use a secret key, which is locally stored at the device, to decrypt the configuration information received from the remote system through the interface [para. 0015, 0044, 0047-0052, whereas stored in encrypted form and loaded into the IC constitutes the encrypting the configuration information, and subsequent decryption of content using the control words and service keys.]; an encryption mechanism that is configured to encrypt the configuration information using a device key, wherein the device key is locally stored at the device and is different from keys associated with other devices [i.e., para. 0047-0052, whereas service keys based on unique keys constitutes the 'different from keys associated with other devices']: and a configuration mechanism that is configured to store the encrypted configuration information in a non-volatile configuration store associated with the device [i.e., para. 0047-0052, whereas stored in encrypted form and loaded into the IC constitutes the encrypting the configuration information]; and a one-time programmable memory within the device for storing the device key

and the secret key wherein the one-time programmable memory can be programmed only once and cannot be reprogrammed [i.e., para. 0015, 0044, 0047-0052, 0064, whereas the "unique key programmed at manufacture… written only once" constitutes "the device key is stored in one-time programmable memory within the device"]: whereby the encrypted configuration information contained in the non-volatile configuration store cannot be used with another device [i.e., para. 0047-0052, whereas service keys based on unique keys constitutes the 'different from keys associated with other devices']."

17. Claim 24 ***additionally recites*** the limitation that; "The apparatus of claim 23, further comprising a content screening mechanism that is configured to use the configuration information to control access to a stream of content in order to facilitate subscriber management.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0026-0036, 0044, 0047-0052, whereas "copy management… ", and entitlement control / management constitutes 'subscriber management".).

18. Claim 25 ***additionally recites*** the limitation that; "The apparatus of claim 23 further comprising a validation mechanism that is configured to use a public key of the remote system to validate that the configuration information was digitally signed by a corresponding private key belonging to the remote system.". The teachings of Candelore suggest such limitations (i.e., para. 0015, 0044, 0047-0052, 0064, whereas "The service key is unit key encrypted. It may be a public asymmetric key or secret symmetric key" constitutes the "using a public key of the remote system…" using the associated control words and service keys, whereas the public key aspect is clearly involving the authentication of the device insofar as it inherently a characteristic of such a system in order to assure proper downloadable content to legitimate subscribers.).

Conclusion

19. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100